

Detection of Denial-of-Service Attacks Based on Computer Vision Techniques

A Thesis Submitted for the Degree of
Doctor of Philosophy

By

Zhiyuan Tan

in

Faculty of Engineering and Information Technology
UNIVERSITY OF TECHNOLOGY, SYDNEY
AUSTRALIA
19TH DECEMBER 2013

© Copyright by Zhiyuan Tan, 2013

CERTIFICATE

Date: **19th December 2013**

Author: **Zhiyuan Tan**

Title: **Detection of Denial-of-Service Attacks Based on
Computer Vision Techniques**

Degree: **Ph.D.**

I certify that this thesis has not already been submitted for any degree and is not being submitted as part of candidature for any other degree.

I also certify that the thesis has been written by me and that any help that I have received in preparing this thesis, and all sources used, have been acknowledged in this thesis.

Signature of Author

Acknowledgements

I am greatly indebted to my supervisor, Xiangjian He for his continuous encouragement, advice, help and invaluable suggestions. He is such a nice, generous, helpful and kindhearted person. I feel really happy, comfortable and unconstrained with him during my PhD study. I owe my research achievements to his experienced supervision. Many thanks are also due to my co-supervisors, Priyadarsi Nanda and Ren Ping Liu for their valued suggestions and constant support, and for the numerous conversations with them. I gratefully acknowledge the useful discussions with Aruna Jamdagni and Qiang Wu. I appreciate the travel support for attending the international conferences which I received from the Faculty of Engineering and IT and the Vice-Chancellor's Conference Fund. I wish to thank my fellow research students and the staff of the school, especially those people listed below for providing various assistance for the completion of this research work.

- Wenjing Jia, Min Xu, Yida Xu, Massimo Piccardi, Doan B. Hoang, Mao Lin Huang, Valerie Gay, Jinjun Chen, Karla Felix Navarro, Ruo Du, Cao Zeng, Sheng Wang, Muhammad Abul Hasan, Man To Wang, Mohammed Ambu Saidi, Ava Bargi, Thawatchai Chomsiri, Mian Ahmad Jan, Yi Wan and Minqi Li.

I would like to thank my wife, Shanshan, for her understanding and assistance. I also thank my parents for the freedom to study for the long time necessary to complete postgraduate studies. This thesis could not have been completed without the support and encouragement of my mother-in-law. My special thanks go to my best friends, Ming Deng and Susan Lai for their continuous care and wishes.

Last but not least, the financial assistance of a University of Technology Sydney International Research Scholarship and a CSIRO ICT Centre Top-up Scholarship is gratefully appreciated.

To My Family

Table of Contents

Table of Contents	vii
List of Tables	viii
List of Figures	x
Abbreviation	xiii
Abstract	1
1 Introduction	6
1.1 Background and Motivation	6
1.1.1 Denial-of-Service Attack Mechanisms	7
1.1.2 Denial-of-Service Attack Framework	13
1.1.3 Schemes of Defence	15
1.2 Objectives	17
1.3 Contribution and Novelty	18
1.4 Structure	19
2 Related Works	21
2.1 DoS Attack Detection	21
2.1.1 Detection Method	22
2.1.2 Audit Source Location	23
2.1.3 Detection Framework	24
2.2 Network Anomaly-based Detection	28
2.3 Earth Mover's Distance	34
2.3.1 Earth Mover's Distance Approaches	35
2.3.2 Applications of Earth Mover's Distance in Network Security .	36
2.4 Summary	38

3	A System Framework for Denial-of-Service Attack Detection	39
3.1	Detection Mechanisms	39
3.1.1	Network Traffic Monitoring at Destination Network	40
3.1.2	Attack Detection Based on Individual Traffic Records	40
3.1.3	Multivariate Correlation Analysis	46
3.1.4	Anomaly-based Intrusion Detection	47
3.1.5	Traffic Classification Based on Computer Vision Techniques	47
3.2	Detection System Framework	49
3.3	Summary	51
4	Multivariate Correlation Analysis Based on Euclidean Distance Map	52
4.1	Multivariate Correlation Analysis Approach	54
4.1.1	Multivariate Correlation Extraction	54
4.1.2	Example and Discussion	57
4.2	Network Intrusion Detection Using Multivariate Correlation Analysis Based on Euclidean Distance Map	59
4.2.1	Framework	59
4.2.2	Training Phase	61
4.2.3	Test Phase	63
4.3	Evaluation on the Multivariate Correlation Analysis Based on Eu- clidean Distance Map	64
4.3.1	Evaluation Datasets	65
4.3.2	Experimental Data for Evaluation	66
4.3.3	Evaluation on Network Traffic Characterisation	66
4.3.4	Evaluation on DoS Attack Detection	72
4.4	Computational Complexity	81
4.5	Summary	83
5	Multivariate Correlation Analysis Based on Triangle Area Map	85
5.1	Multivariate Correlation Analysis Approach	87
5.1.1	Multivariate Correlation Extraction	88
5.1.2	Example and Discussion	90
5.2	Network Intrusion Detection Using Multivariate Correlation Analysis Based on Triangle Area Map	94
5.2.1	Framework	94
5.2.2	Training Phase	97
5.2.3	Test Phase	100
5.3	Evaluation on the Multivariate Correlation Analysis Based on Triangle Area Map	101

5.3.1	Experimental Data for Evaluation	102
5.3.2	Process of Evaluation	102
5.3.3	Evaluation Using the Original Data	103
5.3.4	Evaluation Using the Normalised Data	109
5.3.5	Performance Comparisons	113
5.4	Computational Complexity and Time Cost Analysis	117
5.5	Summary	120
6	Detection of Denial-of-Service Attacks Based on Computer Vision Techniques	122
6.1	Mathematical Techniques for Network Traffic Data Analysis	125
6.1.1	Principal Component Analysis	125
6.1.2	Multivariate Correlation Analysis	127
6.1.3	EMD- L_1	130
6.2	DoS Attack Detection System	135
6.2.1	General Detection Mechanisms	136
6.2.2	System Framework	137
6.3	Relevant Algorithms	139
6.3.1	Algorithm for Dimensionality Reduction Based on PCA	140
6.3.2	Algorithm for Normal Profile Generation Based on MCA	141
6.3.3	Algorithm for Attack Detection Based on EMD- L_1	144
6.4	System Evaluation	145
6.4.1	Evaluation Metrics	146
6.4.2	Evaluations on Detection Performance	146
6.4.3	Comparison of Performance	152
6.4.4	Analysis on Computational Complexity and Time Cost	154
6.5	Summary	156
7	Conclusions	157
7.1	Summary	158
7.2	Future Work	162
	Bibliography	165

List of Tables

4.1	The Number of Records of Normal Traffic and Various of DoS Attack Traffic	72
4.2	Average Detection Performance of the Proposed Attack Detection System on Original Data against Different Thresholds	76
4.3	Accuracy Achieved by the Proposed Detection System on Original Data against Different Thresholds	78
4.4	Average Detection Performance of the Proposed Attack Detection System Based on Normalised Data against Different Thresholds	79
4.5	Accuracy Achieved by the Proposed Detection System on Normalised Data against Different Thresholds	80
4.6	Performance Comparisons with Different Detection Systems	81
4.7	Computational Complexities of Different State-of-the-art Detection Approaches	83
5.1	Average Detection Performance of the Proposed System on Original Data Against Different Thresholds	107
5.2	Detection Rate and False Positive Rates Achieved by the Proposed System on Original Data	108
5.3	Average Detection Performance of the Proposed System on Normalised Data Against Different Thresholds	112
5.4	Detection Rate and False Positive Rate Achieved by the Proposed System on Normalised Data	113

5.5	Performance Comparisons with Different Detection Approaches . . .	116
5.6	Computational Complexities of Different State-of-the-art Detection Approaches	119
6.1	The Numbers of Principle Components for Various Network Traffic .	148
6.2	The Numbers of Principle Components Using in the Training and Test for Various Network Traffic	149
6.3	False Positive Rates, Detection Rates and Accuracies Achieved by the Proposed System Based on the EDM-based MCA Approach	150
6.4	False Positive Rates, Detection Rates and Accuracies Achieved by the Proposed System Based on the TAM-based MCA Approach	150
6.5	Performance Comparisons with Different Detection Approaches . . .	153
6.6	Computational Complexities of Different State-of-the-art Detection Approaches	155

List of Figures

1.1	IP fragment structure [50]	8
1.2	An example of overlapping IP fragments [50]	9
1.3	Typical architecture of a DDoS attack	13
1.4	Architecture of a DDoS attack using reflectors	14
3.1	A general system framework for denial-of-service attack detection . .	49
4.1	A system framework for denial-of-service attack detection using multi-variate correlation analysis based on Euclidean distance map	60
4.2	An algorithm for normal profile generation based on EDM-based MCA approach.	62
4.3	An algorithm for attack detection based on EDM-based MCA approach.	64
4.4	The EDM of a normal TCP traffic record.	67
4.5	Images of the EDMs of normal TCP traffic record, Land attack record and Neptune attack record.	69
	(a) Normal TCP traffic record	69
	(b) Land attack traffic record	69
	(c) Neptune attack traffic record	69
4.6	Images of EDMs of UDP traffic record and Teardrop attack record. .	70
	(a) Normal UDP traffic record	70
	(b) Teardrop attack traffic record	70
4.7	Images of EDMs of ICMP traffic record, Pod attack record and Smurf attack record.	71

(a)	Normal UDP traffic record	71
(b)	Pod attack traffic record	71
(c)	Smurf attack traffic record	71
4.8	The ROC curves of various types of original DoS attack traffic data .	77
4.9	The ROC curves of various types of normalised DoS attack traffic data	79
5.1	Geometrical structure of features	92
(a)	x_{ex} in an orthogonal 3D feature space	92
(b)	x_{ex} projected on feature subspaces	92
(c)	Projected point $y_{ex,1,2}$ on subspace $\mathbb{S}_{\varepsilon_1\varepsilon_2}$	92
(d)	Projected point $y_{ex,1,3}$ on subspace $\mathbb{S}_{\varepsilon_1\varepsilon_3}$	92
(e)	Projected point $y_{ex,2,3}$ on subspace $\mathbb{S}_{\varepsilon_2\varepsilon_3}$	92
5.2	A system framework for denial-of-service attack detection using multi- variate correlation analysis based on triangle area map	95
5.3	An algorithm for normal profile generation based on TAM-based MCA approach.	98
5.4	An algorithm for attack detection based on TAM-based MCA approach.	100
5.5	Images of the TAMs of normal TCP traffic record, Land attack record and Neptune attack record generated using original data.	104
(a)	Normal TCP traffic record	104
(b)	Land attack traffic record	104
(c)	Neptune attack traffic record	104
5.6	Images of TAMs of UDP traffic record and Teardrop attack record generated using original data.	105
(a)	Normal UDP traffic record	105
(b)	Teardrop attack traffic record	105
5.7	Images of TAMs of ICMP traffic record, Pod attack record and Smurf attacks generated using original data	106
(a)	Normal ICMP traffic record	106
(b)	Pod attack traffic record	106

(c)	Smurf attack traffic record	106
5.8	Images of TAMs of normal TCP traffic record, Land attack record and Neptune attack record generated using normalised data	110
(a)	Normal TCP traffic record	110
(b)	Land attack traffic record	110
(c)	Neptune attack traffic record	110
5.9	Images of TAMs of ICMP traffic, Pod attack record and Smurf attack record generated using normalised data	111
(a)	Normal ICMP traffic record	111
(b)	Pod attack traffic record	111
(c)	Smurf attack traffic record	111
5.10	Images of TAMs of UDP traffic record and Teardrop attack record generated using normalised data	112
(a)	Normal UDP traffic record	112
(b)	Teardrop attack traffic record	112
5.11	The ROC curve for analysing original data	114
5.12	The ROC curve for analysing normalised data	114
6.1	Decompose a flow	133
6.2	The framework for our proposed denial-of-service attack detection system	138
6.3	The algorithm for dimensionality reduction based on the PCA.	140
6.4	The algorithm for normal profile generation based on MCA.	142
6.5	The algorithm for attack detection based on the EMD- L_1	144
6.6	Accumulative variance plots for TCP, UDP and ICMP traffic	147
(a)	Accumulative variance plot for TCP traffic	147
(b)	Accumulative variance plot for UDP traffic	147
(c)	Accumulative variance plot for ICMP traffic	147
6.7	Detection accuracy versus threshold	151

Abbreviation

Abbreviations	Descriptions
ABC	Association Based Classification
ANN	Artificial Neural Networks
AR	Auto-regression
BF	Basic Feasible
bPDM	bivariate Parametric Detection Mechanism
CAT	Change Aggregation Trees
CIDS	Collaborative Intrusion Detection System
CPM	Change-Point Monitoring
CUSUM	Cumulative Sum
DEMD	Differential Earth Mover's Distance
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DR	Detection Rate
EDM	Euclidean Distance Map
EMD	Earth Mover's Distance
EMD- L_1	EMD with L_1 distance
FPR	False Positive Rate
FNR	False Negative Rate
FN	False Negative
FP	False Positive
GDI	Global Defence Infrastructure

Abbreviations	Descriptions
GSAD	Geometrical Structure Anomaly Model
ISP	Internet Service Provider
LDA	Linear Discriminant Analysis
LDSes	Local Detection Systems
LP	Linear Programming
MARS	Multivariate Adaptive Regression Splines
MCA	Multivariate Correlation Analysis
MD	Mahalanobis Distance
MDM	Mahalanobis Distance Map
MIB	Management Information Based
PCA	Principal Component Analysis
PoD	Ping of Death
RBFNN	Radial Basis Function Neural Networks
RePIDS	Real-time Payload-based IDS
ROC	Receiver Operating Characteristic
TAM	Triangle Area Map
TCB	Transmission Control Block
TCP	Transmission Control Protocol
TNR	True Negative Rate
TN	True Negative
TP	True Positive
SIP	Secure Infrastructure Protocol
SNMP	Simple Network Management Protocol
SPRT	Sequential Probability Ratio Test
SVM	Support Vector Machine
UDP	User Datagram Protocol
ICMP	Inter Control Message Protocol

Abstract

A Denial-of-Service (DoS) attack is an intrusive attempt, which aims to force a designated resource (e.g., network bandwidth, processor time or memory) to be unavailable to its intended users. This attack is launched either by deliberately exploiting system vulnerabilities of a victim (e.g., a host, a router, or an entire network) or by flooding a victim with large volume of useless network traffic. Since 1990s, DoS attacks have emerged as a type of the most severe network intrusive behaviours and have posed serious threats to the infrastructures of computer networks and various network-based services.

This thesis aims to provide an intelligent and effective solution for DoS attack detection. Unlike the related works based on machine learning and statistical analysis, this thesis suggests to treat network traffic records as images and to redefine the DoS attack detection problem as a computer vision task.

To achieve the aforementioned objectives, this thesis first conducts a detailed literature review on the state of the art in DoS attack detection. Then, it analyses and chooses the most appropriate mechanisms for DoS attack detection. Afterwards, it designs a general system framework for DoS attack detection with respect to the chosen mechanisms. Furthermore, two Multivariate Correlation Analysis (MCA) approaches are proposed based on two techniques, namely Euclidean distance and triangle area.

These two proposed MCA approaches provide accurate description for network traffic records and facilitate conversion of network traffic into the respective images.

In addition, this thesis proposes a DoS attack detection system, in which the images of network traffic are served as the observed objects and the task of DoS attack detection is reformulated as a computer vision problem, namely image retrieval. This proposed DoS attack detection system applies a widely used dissimilarity measure, namely the Earth Mover's Distance (EMD), to object classification. The EMD takes cross-bin matching into account and provides a more accurate evaluation on the dissimilarity between distributions than some other well-known dissimilarity measures, such as Minkowski-form distance L_p and χ^2 statistics. The merits of the EMD facilitate the capability of our proposed system with effective detection.

Last but not least, our intelligent and effective solutions, including the two proposed MCA approaches and the EMD-based DoS attack detection system, are evaluated using the KDD Cup 99 dataset. The evaluation results illustrate that our proposed MCA approaches provide accurate characterisation for network traffic, and the proposed detection system can detect unknown DoS attacks and outperforms two state-of-the-art approaches.

Papers from the Thesis

Papers Appearing in LNCS Series

- [1] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Multivariate Correlation Analysis Technique Based on Euclidean Distance Map for Network Traffic Characterization, Information and Communications Security, LNCS, Vol.

7043/2011, pp.388-398. Springer Berlin Heidelberg New York. ISBN: 978-3-642-25242-6.

- [2] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. Neural Information Processing, LNCS, Part 3, Vol. 7064/2011, pp.756-765. Springer Berlin Heidelberg New York. ISBN: 978-3-642-24964-8.

- [3] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, W. Jia, W. Yeh, A Two-tier System for Web Attack Detection Using Linear Discriminant Method, Information and Communications Security, LNCS, Vol. 6476/2010, pp.459-471. Springer Berlin Heidelberg New York. ISBN: 978-3-642-17649-4.

Refereed Journal Articles

- [4] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Detection of Denial-of-Service Attacks Based on Computer Vision Techniques, IEEE/ACM Transactions on Networking (IEEE/ACM ToN), Submitted for review on 25th May 2013.
- [5] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis, IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS), Available online, 03/05/2013. DOI: 10.1109/TPDS.2013.146.
- [6] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, RePIDS: A Multi Tier Real-Time Payload-Based Intrusion Detection System, Computer Networks, 57(3) 2013, pp. 811-824. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2012.10.002.

- [7] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Mahalanobis Distance Map Approach for Anomaly Detection of Web-based Attacks, *Journal of Network Forensics*, Volume 2 Issue 2, 2010, pp.25-39.

Refereed Conference Papers

- [8] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Evaluation on Multivariate Correlation Analysis Based Denial-of-Service Attack Detection System, 1st International Conference on Security of Internet of Things (SecurIT 2012), Kerala, India, 17-19 August, 2012.
- [9] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, R.Liu, Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection, 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), Liverpool, UK, 25-27 June 2012.
- [10] Zhiyuan Tan, A. Jamdagni, X. He, P. Nanda, Network Intrusion Detection Based on LDA for Payload Feature Selection, IEEE Globecom 2010 Workshop on Web and Pervasive Security (WPS 2010), Miami, USA, December 6 - 10, 2010, pp.1590-1594. IEEE Communication Society.
- [11] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Mahalanobis Distance Map Approach for Anomaly Detection of Web-based Attacks, The 8th Australian Information Security Management Conference, Perth, Australia, November 30 - December 2, 2010, pp.8-17.
- [12] A. Jamdagni, Zhiyuan Tan, R. Liu; P. Nanda, X. He, Pattern Recognition Approach for Anomaly Detection of Web-based Attacks, The proceedings of

the seventh annual CSIRO ICT Centre Science and Engineering Conference, CSIRO, Australia, November, 2010.

- [13] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Intrusion Detection Using GSAD Model for HTTP Traffic on Web Services, 6th International Wireless Communications and Mobile Computing Conference (IWCMC 2010), Caen, France, June 28 - July 2, 2010, pp. 1193-1197. ACM.
- [14] A. Jamdagni, Zhiyuan Tan, P. Nanda, X. He, R. Liu, Intrusion Detection Using Geometrical Structures, 4th International Conference on Frontier of Computer Science and Technology (FCST 2009), Shanghai, China, December 17-19, 2009, pp. 327 - 333. IEEE Computer Society.
- [15] A. Jamdagni, Zhiyuan Tan, R. Liu; P. Nanda, X. He, A Frame Work for Geometrical Structure Anomaly Detection Model, The proceedings of the sixth annual CSIRO ICT Centre Science and Engineering Conference, CSIRO, Australia, November 11, 2009.

Other Publications

- [16] Zhiyuan Tan, Linear Discriminant Analysis Based Feature Selection for Network Intrusion Detection, UTS: FEIT Research Showcase 2010, University of Technology Sydney, Australia, June 2, 2010